



# Cyber Threat Briefing



Anchorage Division  
Scott A. Sandback

This briefing is UNCLASSIFIED in it's entirety



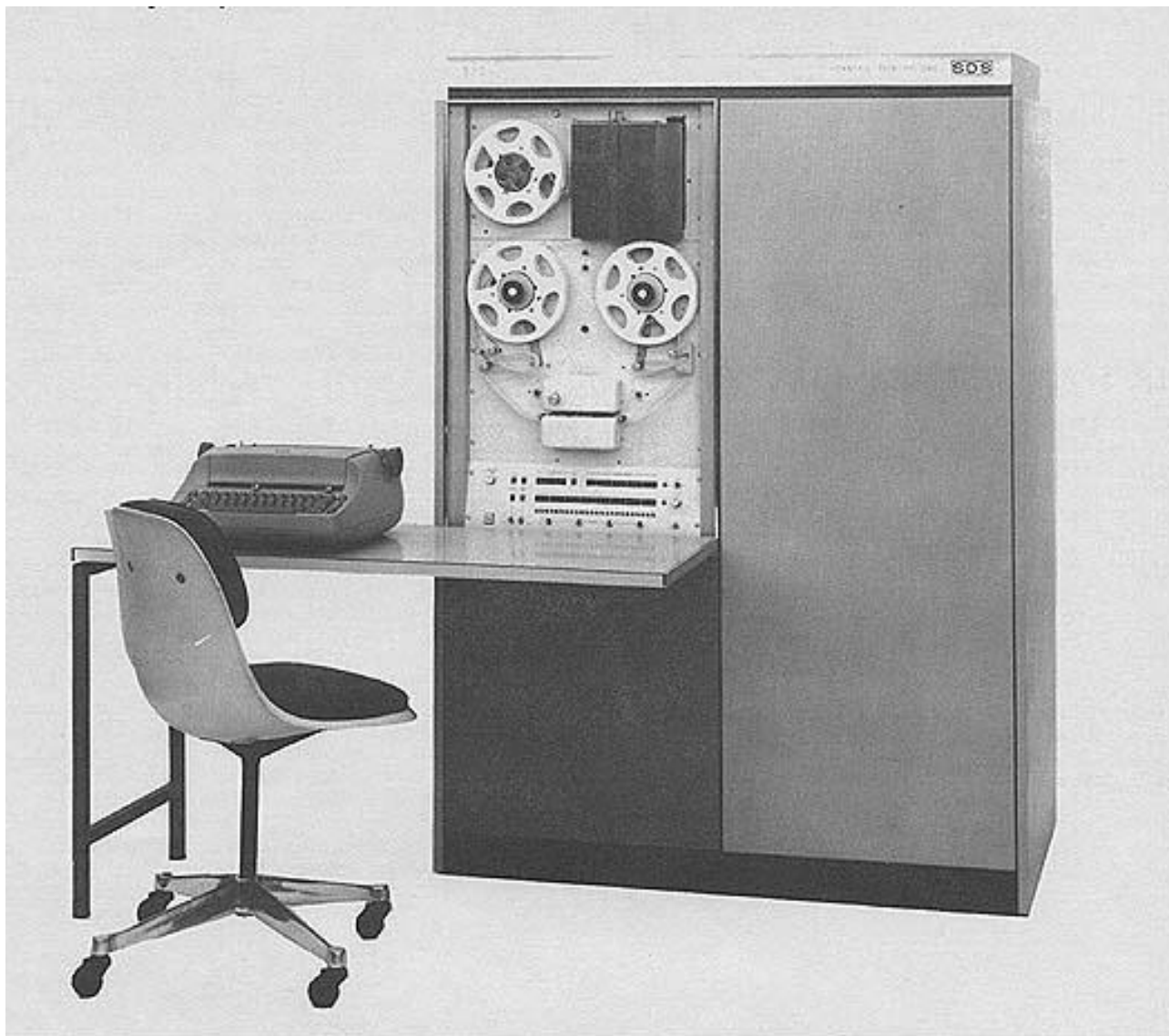
# Agenda

- Introduction
- Threat/Vulnerability/Risk
- Actors
- Motives
- Tools
- Indicators
- Predictions
- Summary





# Introduction





# Introduction





What, me worry?





# The Growing Cyber Threat

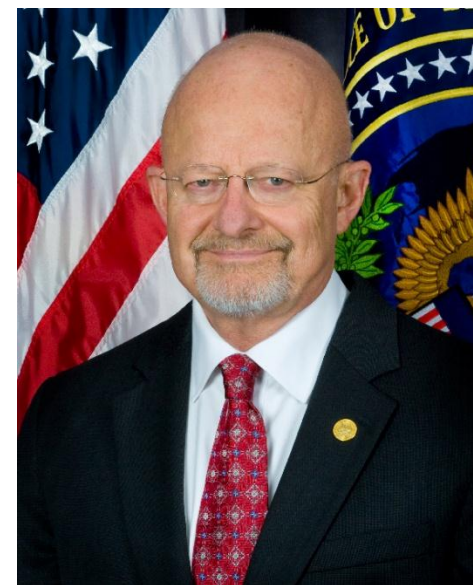


“I do not think today it [cyber] is necessarily the number one threat, but it will be tomorrow...”

-Director of the Federal Bureau of Investigation, Robert S. Mueller III, during his testimony on Capitol Hill to the Senate Intelligence Committee on 31 January, 2012.

“Chinese theft of U.S. intellectual property through hacking and computer espionage is the greatest pillaging of wealth in history,”

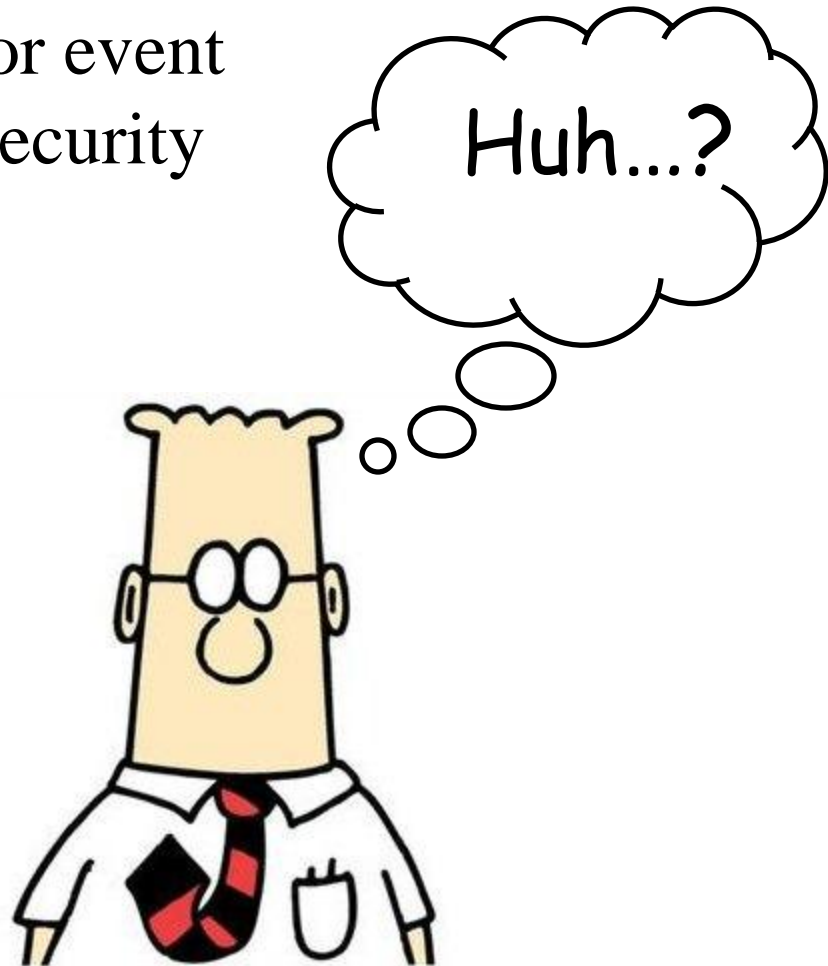
-Director of National Intelligence, James R. Clapper during his testimony on Capitol Hill to the Senate Intelligence Committee on 31 January, 2012.





# Threat

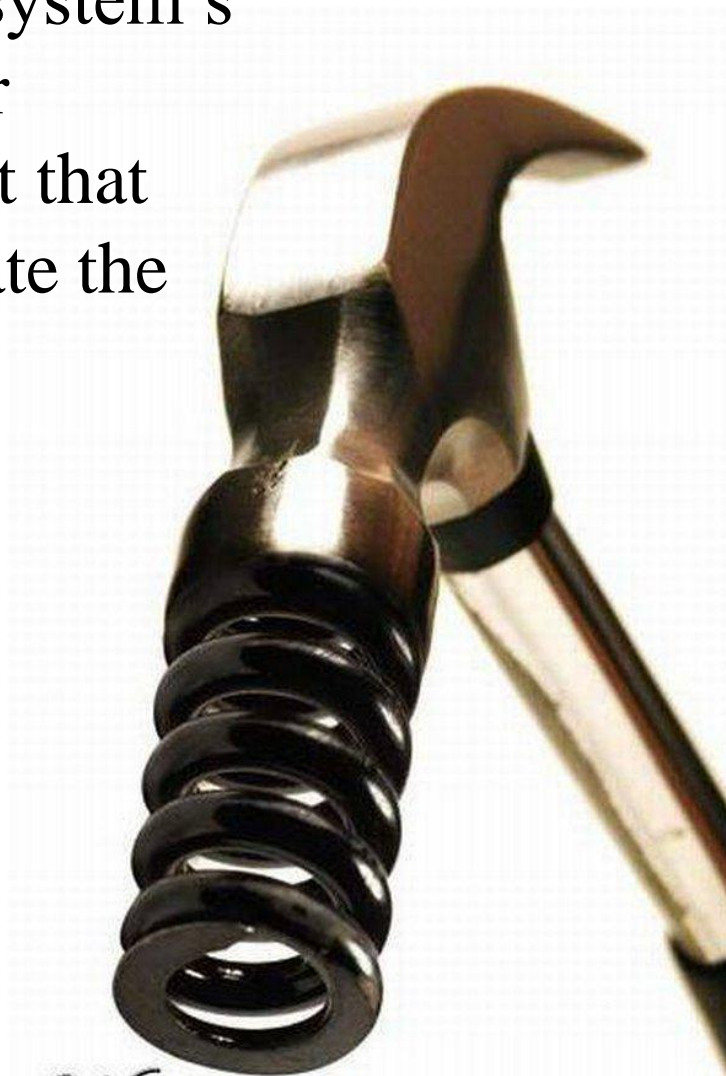
“A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.”





# Vulnerability

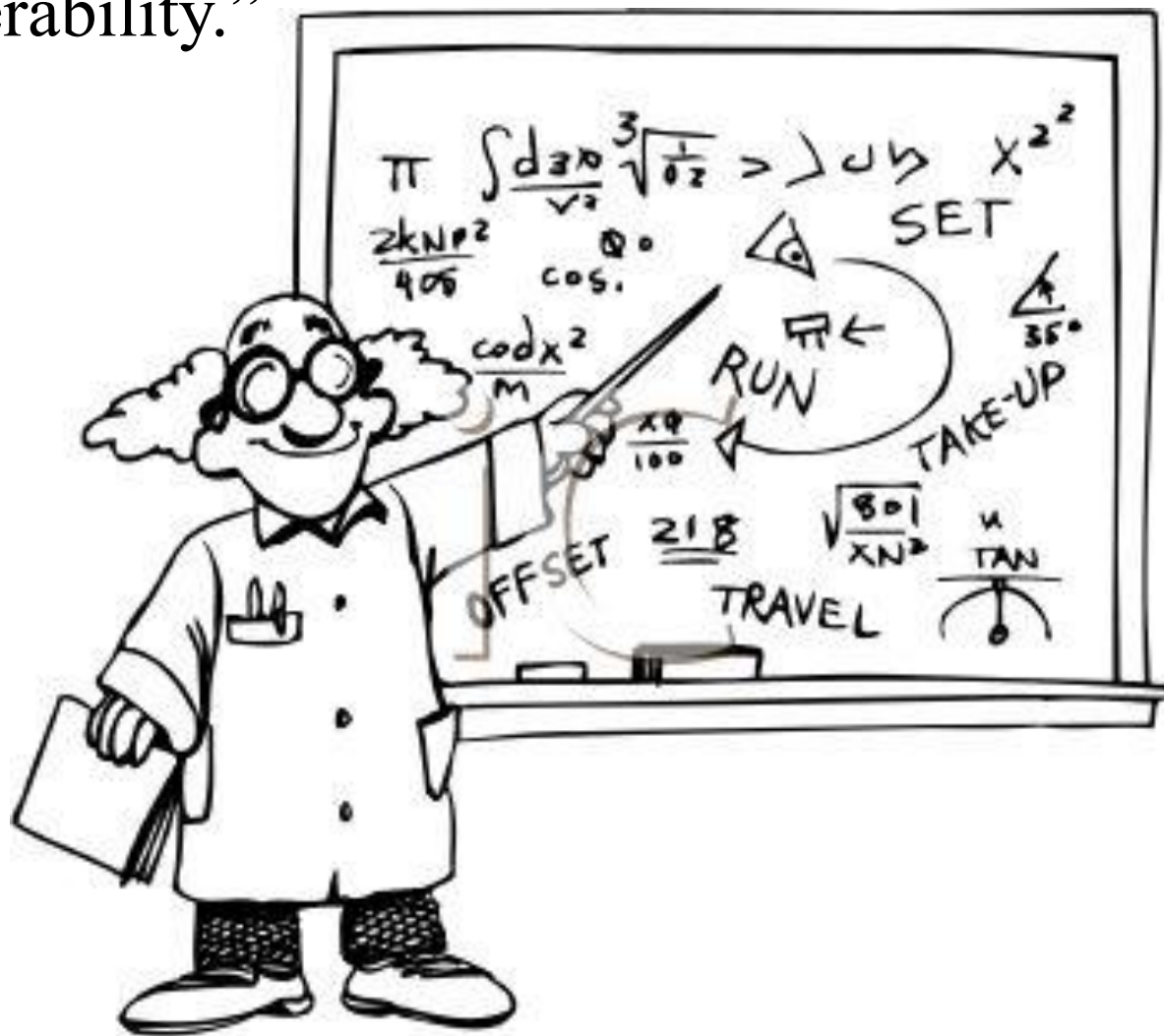
“A flaw or weakness in a system’s design, implementation, or operation and management that could be exploited to violate the system’s security policy.”





# Risk

“The product of the level of threat with the level of vulnerability.”





# The Actors (a.k.a. The Threat)





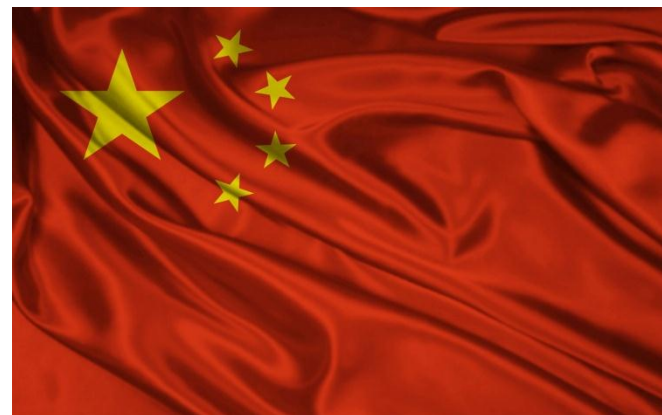
# The People's Republic of China

- Advanced Persistent Threat (APT)
- Tenacious in achieving objectives
- Motivated by massive appetite for secrets and intellectual property

White Paper



- Dedicating a LOT of resources



## Global Energy Cyberattacks: "Night Dragon"

By McAfee® Foundstone® Profess  
February 10, 2011

White Paper



### Revealed: Operation Shady RAT

By Dmitri Alperovitch, Vice President, Threat Research, McAfee

An investigation of targeted intrusions into more than 70 global companies, governments, and non-profit organizations during the last five years

“Chinese theft of U.S. intellectual property through hacking and computer espionage is the greatest pillaging of wealth in history,”

-DNI, James R. Clapper





# Russia

- Majority of cyber activities criminal in nature
- Financially motivated
- Allegations of cyber attacks against political opponents



## News Front Page



Africa  
Americas  
Asia-Pacific  
**Europe**  
Middle East  
South Asia  
UK  
Business  
Health  
Science & Environment  
Technology  
Entertainment  
Also in the news

Video and Audio

Last Updated: Thursday, 17 May 2007, 15:21 GMT 16:21 UK

[E-mail this to a friend](#)

[Printable version](#)

## Estonia hit by 'Moscow cyber war'

**Estonia says the country's websites have been under heavy attack for the past three weeks, blaming Russia for playing a part in the cyber warfare.**

Many of the attacks have come from Russia and are being hosted by Russian state computer servers, Tallinn says. Moscow denies any involvement.



Estonia says many state websites have been affected

Estonia says the attacks began after it moved a Soviet war memorial in Tallinn. The move was condemned by the Kremlin.

A Nato spokesman said the organisation was giving Estonia



**SC eConference: PCI compliance | March 20 &**

SC Magazine > News > Russia confirms involvement with Estonia DDoS attacks

## Russia confirms involvement with Estonia DDoS attacks

Chuck Miller March 12, 2009

[PRINT](#) [EMAIL](#) [REPRINT](#) [PERMISSIONS](#) [TEXT: A|A|A](#)

[Tweet](#) 2

The long-rumored perpetrators of **DDoS attacks** during the 2007 conflict between Russia and Estonia were members of a youth group with ties to the Kremlin, a Russian State Duma deputy, Sergei Markov, confirmed to a number of news outlets.

The DDoS claim was made by an activist Konstantin Goloskokov, a member of

**RELATED ARTICLES**  
- Cyberspace nature of war  
- Student first attack on Kremlin  
- Hackers: G



# Iran

- Developing both an intelligence collection capability and a strike capability
- Relatively unsophisticated – but learning fast



- Learned many lessons from Stuxnet
- Perceives Stuxnet as a cyber WMD



# Hacktivism

- 2011 was “The Year of the Hacktivist”
- Motivation varies, but common theme is obtaining media coverage of their cause/prowess/story
- International as well as domestic
- Attacks often triggered by media coverage of hot button issue(s)





# Criminals

- Cyber crimes
- Cyber facilitated crimes
- Financially motivated
- Expertise varies from silly to extremely good
- Get in, get out, get gone



Dear Citibank valued member

Due to concerns, for the safety and integrity of the online banking community we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive members, frauds and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result in account suspension. This is a final warning.



Dear valued customer of TrustedBank,

We have received notice that you have recently attempted to withdraw the following amount from your checking account while in another country: \$135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

<http://www.trustedbank.com/general/custverifyinfo.asp>

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,  
TrustedBank



# Hobbyists and Nerds (i.e. “Script Kiddies”)

- Once upon a time...
- Motivated by ego
- Now, technical knowledge not required to have impact
- The Accidental Terrorist
- Do not confuse lack of expertise with inability to cause grief...





# Insiders

- Varies from accidental incidents...
- ... to deliberate sabotage....
- ... or even espionage....
- And they are already “inside the wire”





# Tools and Techniques



## SOCIAL ENGINEERING

The clever manipulation  
of the natural human  
tendency to trust.



TROJAN



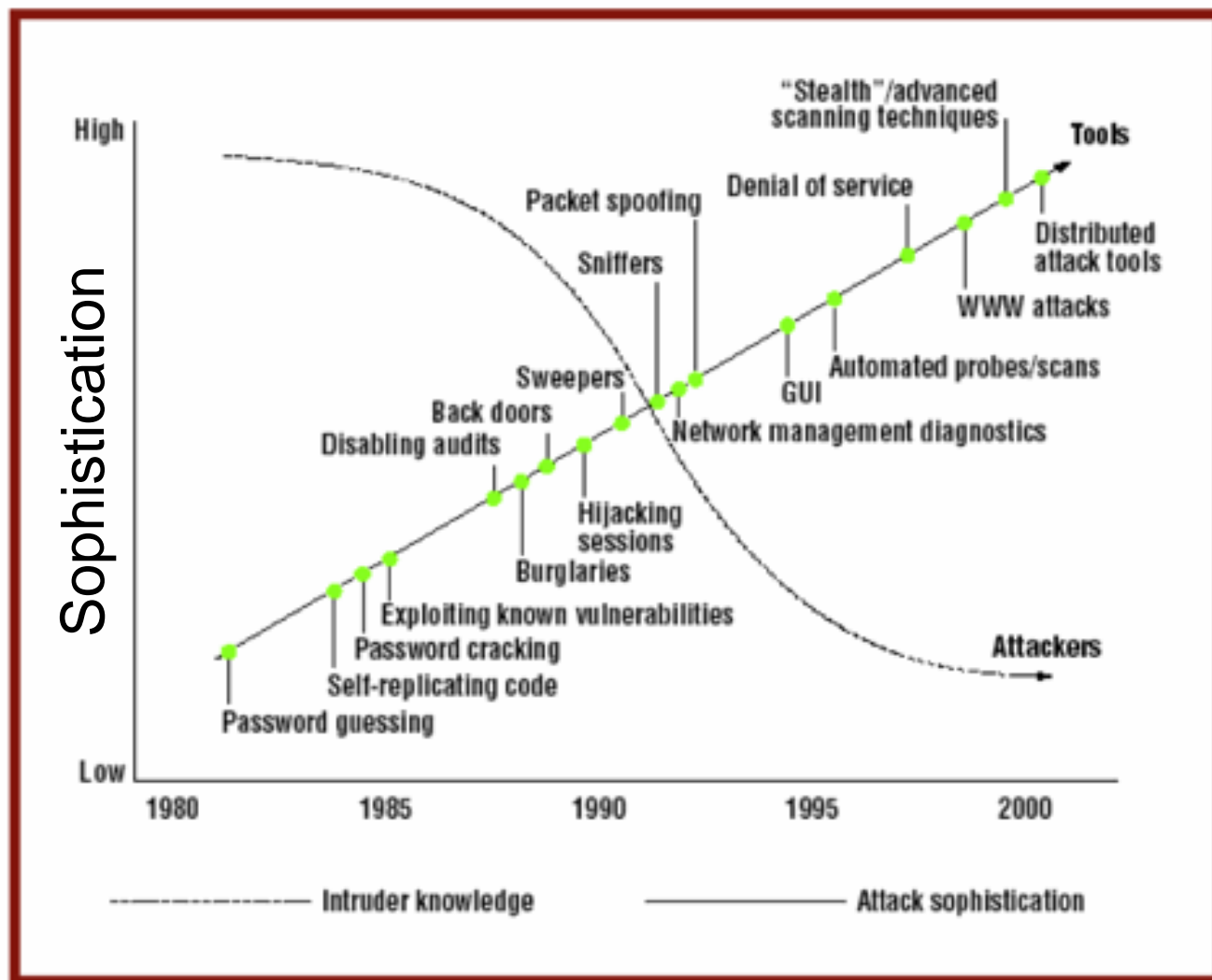
VIRUS



WORM



# Evolving Risk



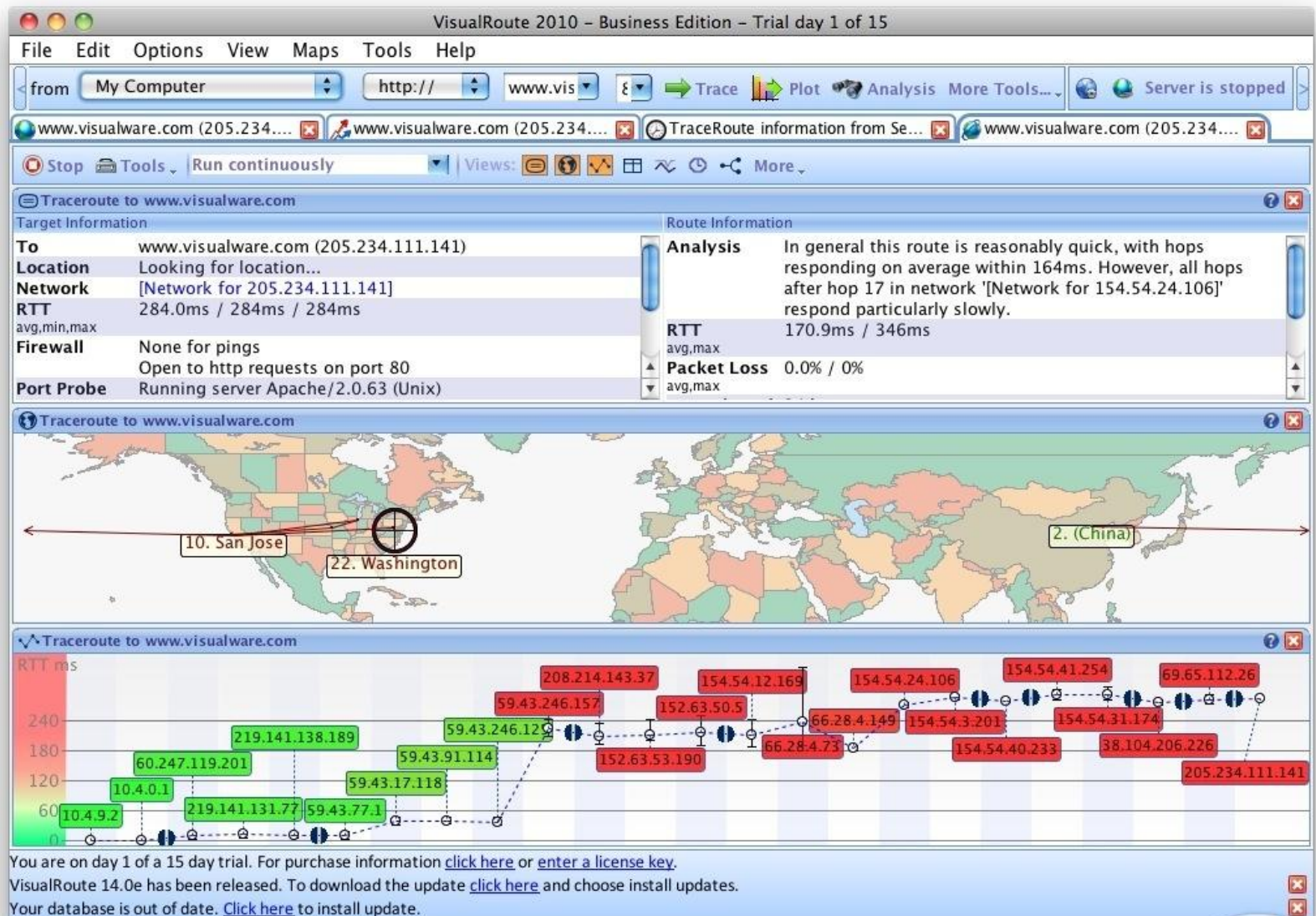


# Physical versus Digital access



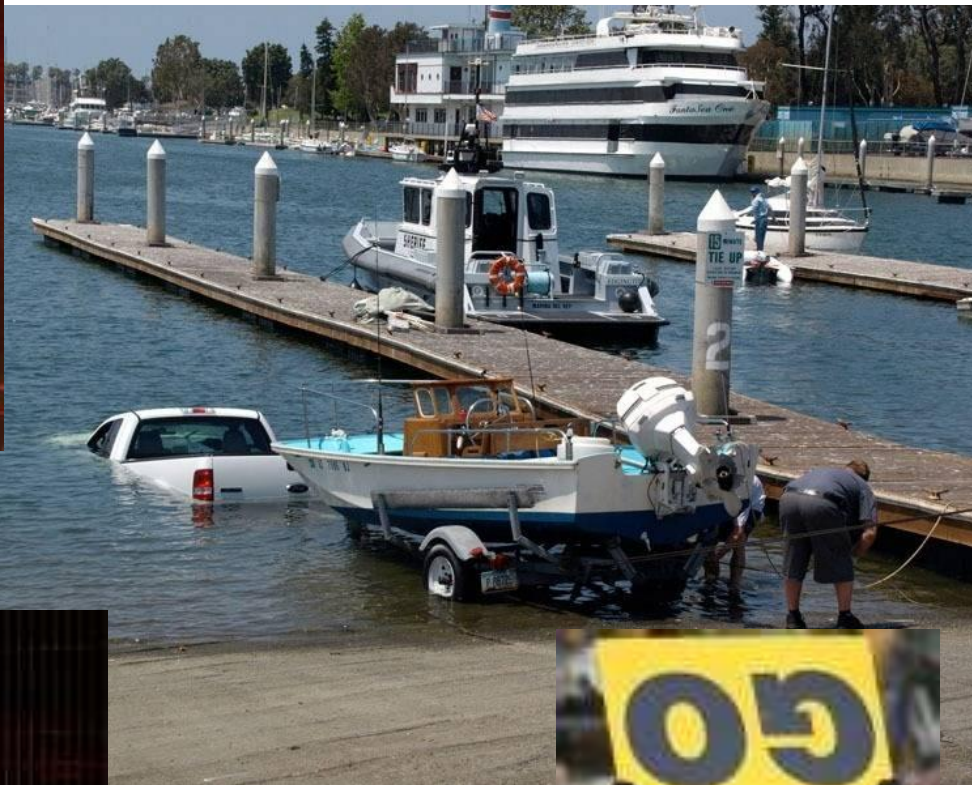


# Physical versus Digital access





# Indicators (...something isn't quite right...)



- Logs
- Logs
- Logs





# What lies ahead...





# Trickery...





# ... and Complacency



## The Internet Crime Complaint Center's (IC3) October/November/December 2011 Trend Analysis and Intelligence Brief

### Popular Passwords

Sharing passwords among users in a workplace is becoming a common theme to continue the flow of operations. Users have prioritized convenience over security when establishing passwords.

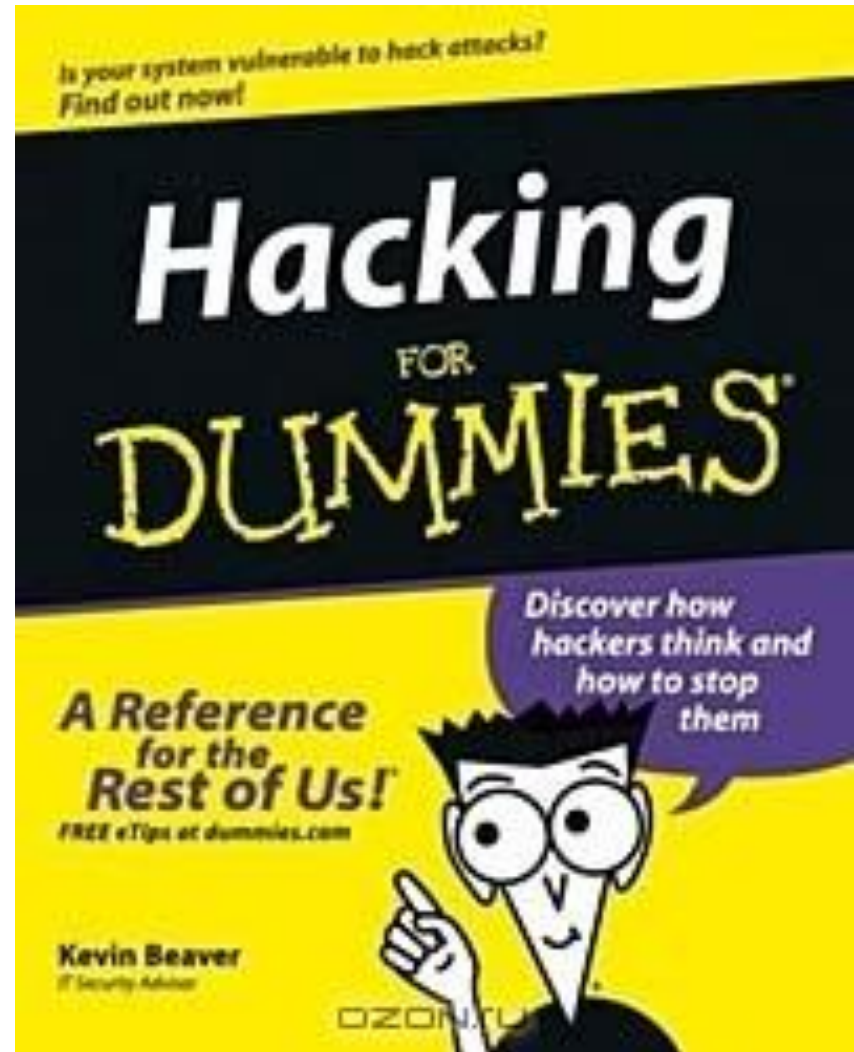
The top 25 common passwords:

- |             |              |              |
|-------------|--------------|--------------|
| 1. password | 10. dragon   | 19. shadow   |
| 2. 123456   | 11. baseball | 20. 123123   |
| 3. 12345678 | 12. 111111   | 21. 654321   |
| 4. qwerty   | 13. iloveyou | 22. superman |
| 5. abc123   | 14. master   | 23. qazwsx   |
| 6. monkey   | 15. sunshine | 24. michael  |
| 7. 1234567  | 16. ashley   | 25. football |
| 8. letmein  | 17. bailey   |              |
| 9. Trustno1 | 18. passw0rd |              |



# Script Kiddies and Wannabes

- Not going away





# E-mail scams



Citi Alerting Service  
**Unauthorized Access**

- Also not going away...
- ... and they are getting better...

---

## Unauthorized Access Notice

We recently have determined that different computers have logged on to your Online Banking account and multiple password failures were present before logons.

We now need to re-confirm your account information with us.

If this is not completed by **November 17, 2010** we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes.

We thank you for your cooperation in this matter.

Please [click here](#) immediately to verify your identity and automatically reverse the change.

## E-mail Security Zone

At the top of this message, you'll see an E-mail Security Zone. Its purpose is to help you verify that the e-mail was indeed sent by Citibank. If you have questions, please call 1-800-374-9700. To learn more about fraud visit Citibank.com and click "Security" at the bottom of the screen

**ABOUT THIS MESSAGE** Please do not reply to this Customer Service e-mail. For account-specific inquiries, kindly call 1-800-374-9700 (TTY: 1-800-788-0002) or visit [citibankonline.com](http://citibankonline.com).



# Other online vices...



- Log Out *Anastasia* DATE.COM
- |  |  |               |
|--|--|---------------|
|  | <b>Galina</b><br>Age: 24<br>Odessa, Ukraine    | ONLINE<br>★ > |
|  | <b>Ekaterina</b><br>Age: 22<br>Odessa, Ukraine | ONLINE<br>★ > |
|  | <b>Viktoria</b><br>Age: 25<br>Kharkov, Ukraine | ONLINE<br>★ > |
|  | <b>Antonina</b><br>Age: 24<br>Kiev, Ukraine    | ONLINE<br>★ > |
|  | <b>Anna</b><br>Age: 29<br>Odessa, Ukraine      | ONLINE<br>★ > |
- androidzoom.com



# Mobile devices

- Emerging threat
- Airborne virus





# Phishing



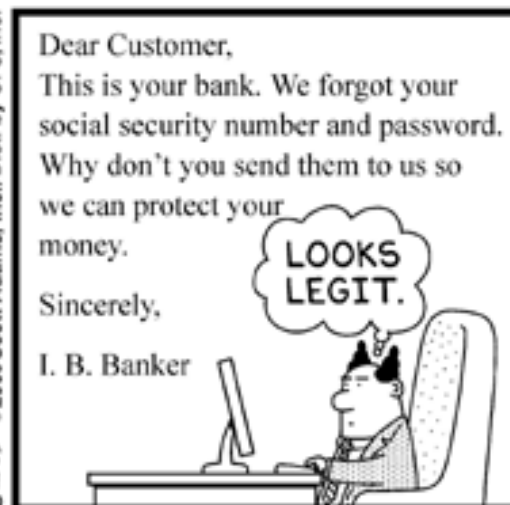
- Still works



www.dilbert.com scottadams@aol.com



8-12-05 © 2005 Scott Adams, Inc./Dist. by UFS, Inc.



© Scott Adams, Inc./Dist. by UFS, Inc.



# Cyber Attack in a box

1. ENTER TARGET ADDRESS (OR IP ADDRESS IF YOU KNOW BELOW)
2. PRESS LOCKON! THIS WILL GIVE YOU THE "SELECTED TARGET" IP INFORMATION

3. TCP: GOOD FOR MOST USE FOR MOST ATTACKS  
HTTP: USE FOR MOST ATTACKS  
UDP: STRONG. WILL SLOW DOWN COMPUTER, BEST TIMES TO USE IS IF THE SITE EXPECTS AN ATTACK
4. PUT A VALUE BETWEEN 100-1000 AVERAGE. HIGHER NUMBER MORE STRENGTH
5. PRESS WHEN READY TO ATTACK!

Low Orbit Ion Cannon | When harpoons, air strikes and nukes fail | v.1.0.0.0

**Low Orbit Ion Cannon**

NON-TRACEABLE  
= USE WITH MANY PEOPLE, WILL TAKE OUT FULL SITES

YOU'LL NEED .NET FRAMEWORK, GOOD CHANCE YOU HAVE THAT ALREADY, IT'S NEEDED FOR A LOT OF SHIT. IF YOU DON'T HAVE IT, GET IT AT MICROSOFT

**DON'T GIVE THIS PROGRAM TO COMPLETE IDIOTS!**

Praetox.com

1. Select your target

URL:

IP:

2. Ready?

IMMA CHARGIN MAH LAZER

Selected target

**71.18.227.199**

3. Attack options

Timeout: 9001

HTTP Subsite: /

TCP / UDP message: You have been hack'd

Port: 80

Protocol: **UDP**

Threads: 750

Wait for reply: ☒

Attack status

Idle Connecting Requesting Downloading Downloaded **Requested** Failed


17395574

WHAT IS THIS SHIT? = LOW ORBIT ION CANNON (LOIC) IS A TOOL THAT ALLOWS THE USER(S) TO TAKE OUT WEBSITE OFFLINE VIA A "DISTRIBUTED DENIAL-OF-SERVICE ATTACK" (DDOS ATTACK). IT BASICALLY OVERLOADS THE SERVER AND HENCE CAUSES THE WEBSITE TO CLOSE DOWN. THIS TOOL IS GREAT FOR TAKING OUT SMALL WEBSITES. IN ORDER TO TAKE OUT BIG WEBSITES, YOU WILL NEED A LOT OF PEOPLE DOING THIS AT THE SAME TARGET.

ddos attack: A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. The means to, motives for, and targets of a DoS attack may vary, but it generally consists of the concerted, malevolent efforts of a person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even DNS root servers. High-profile targets often have many users attacking the intended target at the same time. Low-profile targets don't need as many users.



# SCADA



[订阅 ChinaDaily 手机报](#) [Subscribe to free Email Newsletter](#)

[直播客](#) [NEW](#) [环球在线](#) [英语点津](#) [新闻图片](#) [新漫网](#)

[Home](#) | [China](#) | [BizChina](#) | [World](#) | [Opinion](#) | [Sports](#) | [Olympics](#) | [Entertainment](#) | [Lifestyle](#) | [Culture](#) | [Citylife](#) | [Photo](#) | [Forum](#) | [Weather](#)

February 27, 2012

SITE SEARCH:  [GO](#) [Advanced](#)

## WORLD / America

### US video shows hacker hit on power grid

(Agencies)

Updated: 2007-09-27 14:31

Washington - A US government video shows the potential destruction caused by hackers seizing control of a crucial part of the US electrical grid: an industrial turbine spinning wildly out of control until it becomes a smoking hulk and power shuts down.



In this image from video released by the US Department of Homeland Security, smoke pours from an expensive electrical turbine during a March 4, 2007, demonstration by the Idaho National Laboratory, which was simulating a hacker attack against the US electrical grid. [AP]



• [Vietnam bridge collapse kills 52](#)



# Hacktivists

- Expect copycats



**NO, ME !**



**WE ARE  
ANONYMOUS**



**NO, ME !**



**ME ! ME !**



**NO, WE ARE ...**



**NO, WE ARE ...**



**ME ! ME !**



**NO, WE ARE ...**



**NO, WE ARE ...**



**NO, ME !**



# China





# Iran

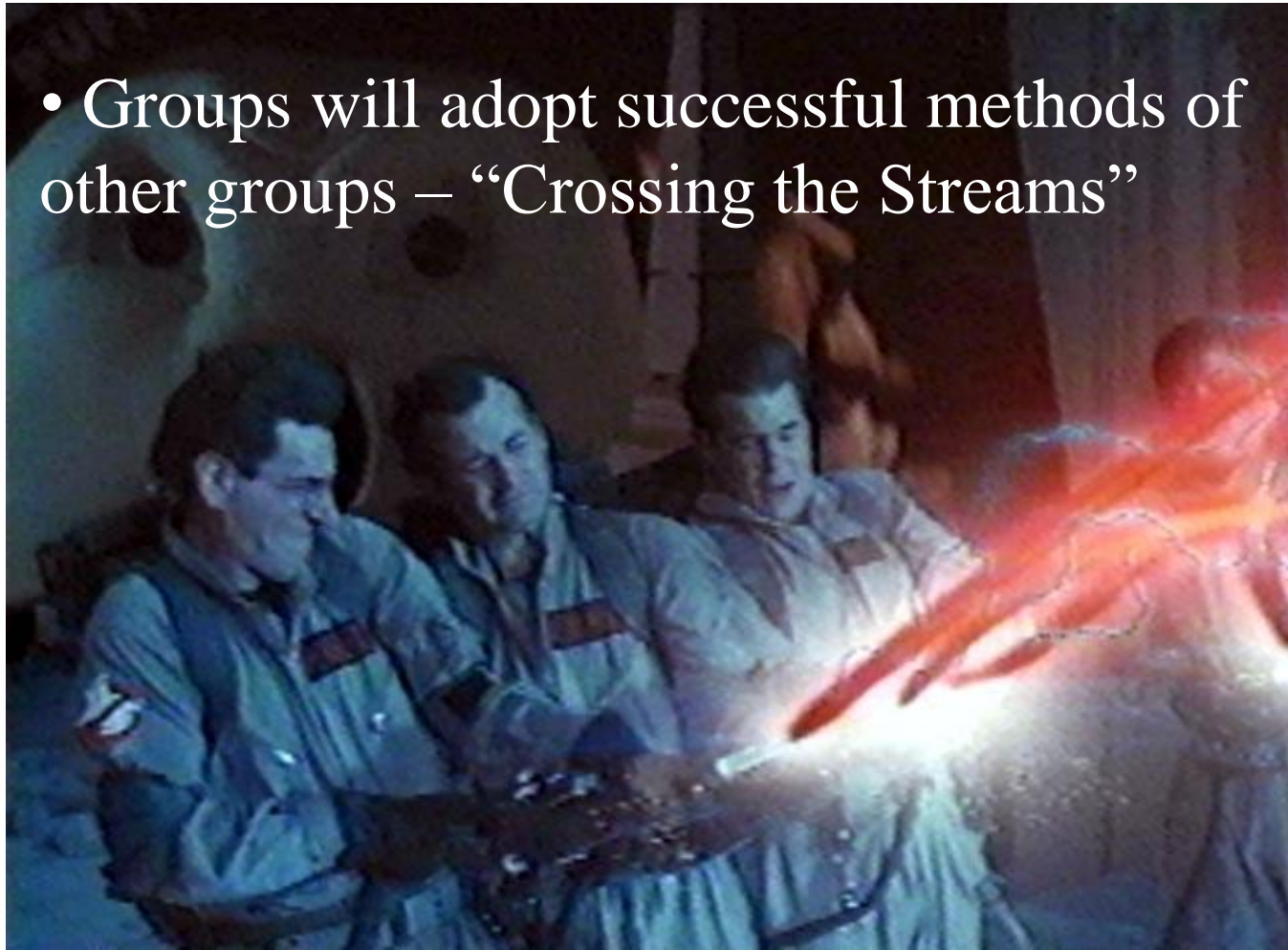
1000110100110100010101001011100010100100100101001  
1001101011101010011101010100101001010011010101010  
0110101010101001010101001010010101001100101010010  
1010110101001001001001010010010110101001010110101  
0110101010100101010100101010100101010011001010101





# Tradecraft

- Groups will adopt successful methods of other groups – “Crossing the Streams”





# Summary

- Threat \* Vulnerability = Risk
- China, Russia, Iran
- Anonymous
- Criminals
- Idiots
- Tools (as opposed to idiots)
- 2012 and beyond





UNCLASSIFIED

UNCLASSIFIED

# Questions?



UNCLASSIFIED